AXALTO SA
Intellectual Property / Propriété Intellectuelle
36-38, rue de la Princesse - B.P. 45
78431 LOUVECIENNES CEDEX - FRANCE
Tel : 33 1 30 08 47 81
Fax : 33 1 30 08 45 24
Email : MMolinari@axalto.com

JC03 Rec'd PCT/PTO 08 JUN 2005

axalto

FAX

MAIL STOP PCT, ATTn : IPEA/US
A l'attention de G. MORSE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Authorized Officer :
G. MORSE Tel : (571) 272-3838

Louveciennes, 1 June 2005

RE / Objet : International Application PCT/IB03/00946In the name of AXALTO SA. Written opinion.
Our Ref./Notre réf.: PCT 76.0728/PR

Dear Sirs,

Following your written opinion dated 21 November 2002, the applicant presents the following argumentation with regard to novelty.

According to the examiner, Roelofsen discloses masking intermediate results (RD1) in input or output (p 9, &1) of at least one critical function (F1-n – Fig. 6) so that the critical function (F1-n) respectively gives in output or receives in input non-masked intermediate results (RDn, p 9, &4 and fig. 6).

However, in claim 1 of the present invention, it is explained masking applies to input or output of said critical function so that the critical function gives in output or receives in input non-masked intermediate result.

The critical function is the function F1-n and in document Roelofsen, input and output are masked. The critical function gives in output and receives in input masked intermediate result.

It is said page 9 in first paragraph of Roelofsen :
"the data present in and between the steps is masked ... They combine the left-hand data LD1 and the right-hand data RD1 ... with a zeroth auxiliary value A0 and a first auxiliary value A1. The results of the combinatory operations DC and EC are left-hand masked data LD'1 and right-hand masked data RD'1 ..."

This method implies as explained page 9 lines 24-26 of Roelofsen:
"In order to remove the auxiliary values Ai prior to the final operation (PP-1), there are provided completing combinatory operations FC and GC ..."

Consequently, the method according to Roelofsen needs to unmask the final result.

In the present invention as disclosed in page 9 lines 6-11, one of the advantage of the present invention is the following : "Thus it is possible to carry a complete DES ... without unmasking in and out." As said in claim 3, it is possible to sequence "replacement functions so as to give non-masked for input and output" of the complete procedure :

Non-masked input → masked intermediate result → non-masked intermediate result → masked intermediate result → non-masked output

As a conclusion, the characteristics of the claims of the present invention are new and inventive in consideration of document Roelofsen.

Very Truly Yours,

Patricia RENAULT
Patent Attorney, Intellectual Property
Tél. : 33 1 30 08 48 33 / Fax : 33 1 30 08 45 24
Email : prenault@axalto.com